REMARKS

The following remarks are made in response to the Office Action mailed November 16, 2005. Claims 1-43 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-43 under 35 U.S.C. § 102(b) as being anticipated by the Ritter U.S. Patent No. 4,979,832.

Independent claims 1, 9, 18, and 31 all include limitations related to providing a keystream and cryptographically combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide the second binary data sequence. Independent claim 1 includes both an encryption combiner and a decryption combiner in a stream cipher cryptosystem. Independent claim 9 includes a cryptographic combiner (which could be an encryption combiner as claimed in dependent claim 10 or a decryption combiner as claimed in dependent claim 11) in a stream cipher cryptosystem. Independent claim 18 claims a method of encrypting a plaintext binary data sequence. Independent claim 31 claims a method of decrypting a ciphertext binary data sequence.

The Ritter patent does not teach or suggestion cryptographically combining a first binary data sequence and the keystream and **performing two sequential non-associative operations** on the first binary data sequence and the keystream to provide a second binary data sequence as included in the limitations of independent claims 1, 9, 18, and 31.

By contrast, the Ritter patent discloses a dynamic substitution combiner and extractor. In the Ritter patent, a plaintext value on input 10 is transformed by substitution 12 into a ciphertext value output 14. A ciphertext value on input 22 is transformed by substitution 24 into the original plaintext value on output 26. Substitution 12 must be invertible to make this work. For example, the substitution table in substitution 12 can be made exactly as large as the number of possible input values 10 and filled sequentially with the possible output values. If no output value appears more than once, substitution 12 will be invertible. Substitution 12 can then be

shuffled or randomized in any number of ways, as long as the values in the table in substitution 12 are re-arranged or permuted, substitution 12 will remain invertible. Typically, substitution 12 is implemented as addressable storage and realized with an electronic memory device, or an addressable area of memory hardware in an electronic digital computer or microprocessor. The substitution changes controller 18 uses both substitution input 10 and combiner substitution changes input 16 to change the content of substitution 12 by way of combiner substitution changes controls 20.

Thus, the Ritter patent dynamic substitution combiner and extractor device is similar to the very complex cryptographic combiner discussed in the Background of Invention section of the present application. As stated in the Background of Invention section of the present application, one example cryptographic combiner in this very complex category is a permutation table combiner, wherein the permutation table is required to have a table the size of the plaintext alphabet. By contrast, each two sequential non-associative operations according to claims 1, 9, 18, and 31 can be implemented with substantially the same complexity as the XOR and other linear combiner operations. As stated in the present application at page 12, lines 14-17, since each combiner operation according to the present invention is substantially the same complexity as the XOR and other linear combiner operations, there is not the extensive expense in time, hardware and/or software resources of conventional very complex combiner operations (such as the dynamic substitution combiner extractor disclosed in the Ritter patent).

Moreover, the Ritter patent actually teaches away from the present invention, as the Ritter patent, at column 3, lines 7-9 states that the "alternative of selecting some other simple Boolean logic function to replace the exclusive-OR combiner does not work." The Examiner states that the Ritter patent teaches an improvement upon exclusive-OR at columns 3, lines 23-62. The Examiner recited text of the Ritter patent, however, actually teaches away from the present invention in further detail to the above-recited text at column 3, lines 7-9. For example, in summarizing its discussion of the background U.S. Patent No. 4,195,196 prior art, the Ritter patent at column 3, lines 55-59 states that the 4,195,196 mechanism is an example of a pseudo-random confusion generator plus conventional exclusive-OR combining, and is "thus susceptible to the plaintext attack, which is a weakness of all exclusive-OR combiners." Thus, the Ritter

patent teaches away from a system or method of cryptographic combining such as claimed in independent claims 1, 9, 18, and 31 which can be implemented with two sequential non-associative operations having substantially the same complexity as the XOR and other linear operations. Instead, the Ritter patent, solves the problem of the susceptibility of the plaintext attack for exclusive-OR combiners with a dynamic substitution combiner and extractor device which is a very complex cryptographic combiner.

By contrast, the cryptographically combining a first binary data sequence in keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence as recited in independent claims 1, 9, 18, and 31 can solve problems of conventional XOR and other linear combiner operations used in cryptosystems, such as having known plaintext being combined with associated ciphertext to reveal the keystream; accidental double encryption to remove the keystream from the combined output bits; or combining two ciphertexts to eliminate the keystream and leaving a combination of the two original plaintext messages. Nonetheless, the stream cipher cryptosystems and methods of independent claims 1, 9, 18, and 31 can be implemented with a minimal increase of resources over conventional XOR and other linear combiner operations as compared to the very complex solution to this problem proposed in the Ritter patent.

In view of the above, Applicant respectfully submits that independent claims 1,9, 18, and 31 are patentably distinct over the Ritter patent, because the Ritter patent does not teach or suggest the stream cipher cryptosystems of independent claims 1 and 9, the method of encrypting of independent claim 18, or the method of decrypting of independent claim 31. In addition, dependent claims 2-8 further define patentably distinct independent claim 1, dependent claims 10-17 further define patentably distinct independent claim 9, dependent claims 19-30 further define patentably distinct independent 18, and dependent claims 32-43 further define patentably distinct independent claim 31. Therefore, these dependent claims are also believed to be patentably distinct over the Ritter patent.

As to the Examiner's remarks at page 7, paragraph 43 of the Office Action, Applicant respectfully points out that Applicant's statements regarding XOR were to provide an illustrative example that the two sequential non-associative operations according to independent claims 1, 9,

18, and 31 can possibly be implemented with XOR. XOR, however, is one of many ways that the two sequential non-associative operations can be implemented according to the limitations of independent claims 1, 9, 18, and 31.

Finally, the Examiner, at page 7, paragraph 43 of the Office Action, urged the Applicant to define independent claims 1, 9, 18, and 31 more specifically as to which two non-associative operations are being used. Applicant, however, respectfully submits that the Ritter patent does not teach or suggestion cryptographically combining a first binary data sequence and the keystream and performing any type of two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence as recited in the limitations of independent claims 1, 9, 18, and 31. Thus, the current language of independent claims 1, 9, 18, and 31 clearly defines limitations not taught or suggested by the Ritter patent.

Therefore, Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 102(b) rejection to claims 1-43, and requests allowance of these claims.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-43 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-43 are respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 50-0471.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Amendment and Response should be directed to Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005. In addition, all correspondence should continue to be directed to the following address:

Dicke, Billig & Czaja
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402

Respectfully submitted,

Kevin R. Driscoll,

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: 2-16-06
PGB:cmj

Patrick G. Billig
Reg. No. 38,080

CERTIFICATE OF FACSIMILE TRANSMISSION: The undersigned hereby certifies that these papers are being transmitted by facsimile to the U.S. Patent and Trademark Office, Fax No. 571-273-8300, on February 16, 2006.

By
Name: Patrick G. Billig